別紙 1

論文の内容の要旨

論文題目	B Methodにおける部品再利用によるソフトウェア合成と高信頼ソフトウェア部品の整備
学位申請者	中村丈洋

本研究では信頼性を定理証明により定性的に評価可能な高信頼ソフトウェアを形式仕様から自動生成する手法の提案を目的としている．また，この手法の実現にあたり課題となる，高信頼部品整備を容易にするため，既存の高信頼ソフトウェアからソフトウェア部品群を自動生成する手法を提案している．

近年のソフトウェアの大規模複雑化に伴い，開発コストの増大と信頼性の低下が問題となっている．高信頼なソフトウェアを容易に開発することはソフトウェア工学の大目標の一つといえる．これに対するドラスティックなアプローチとしては入力仕様や設計から人手によらずコードを生成する自動コード生成が挙げられる．自動コード生成は開発コストの低減や開発期間の短縮だけでなく，人による誤りが混入せず信頼性向上にも寄与する．一方で，生成ソフトウェアの信頼性が部品の信頼性に依存し，高信頼なソフトウェア部品を開発対象ごとに整備する必要があり，このコストが手法適用の妨げとなる．

本研究では数学を基盤としてソフトウェアの信頼性を定性的に保証する形式手法 B Method の枠組みをソフトウェア部品と再利用の自動化に応用することで，高信頼ソフトウェア部品の自動生成とその再利用による新たなソフトウェア開発手法「モデル充足ソフトウェア合成（MSSS）手法」を提案している． B Method は J.R.Abrial らにより提案された形式手法であり，大きな特徴として数学的仕様と命令型言語による実装間の整合性を定理証明に保証できる点である． MSSS 手法ではこの B Method の信頼性保証の枠組みを応用してモデル充足ソフトウェア部品 (MSFC)を定義する．

MSSS 手法は基盤とする数学的仕様の性質上,集合論と述語論理で記述できる範囲内でしかソフトウェアの仕様を記述できず,非同期処理やユーザインタフェースは自動合成の対象外となる．一方で，ソフトウェアの信頼性と MSFC の信頼性を数学的に定義することで， MSSS 手法では部品生成手法とソフトウェア合成手法の信頼性を数学的に定義でき，定性的な評価が可能である．本研究ではソフトウェア部品の生成手法自体に定理証明を適用し，その信頼性を定性的に保証する事を試みた．これにより，細分化モデルの信頼性を保証するのに必要な推論器の性質と，制約条件の抽出条件を定理証明により得られた．ソフトウェア合成についても提案した合成手順で部品の実装間の制約条件の矛盾以外は保証できることを示し，合成結果に矛盾が生じた際の低コストな解決手段を提案している．

MSSS 手法のように数学的判定を必要とする部品自動再利用では膨大な部品群に対して数学的判定を行うため，計算コストの低減が問題となる．本研究ではこの問題に対して，数学的に意味の等しい数学的仕様の字面が一致し，また，含意関係となる字面が完全部分一致となるようモデル細分化手法を提案した．これにより，文字列一致による効率的な部品検索を可能にした．

本研究では MSSS 手法の適用例として銀行口座システムなどに対する MSFC 生成とレンタカーシステムなどの自動合成を行った．これにより生成された MSFC やソフトウェアに対して B Method の証明器を適用し，定義どおりの信頼性が得られることを確認した．ただし， B Method により記述されたソフトウェアは現状では広く公開されておらず，より実践的な手法の適用が今後の課題となる．

近年では，システムの不具合が莫大な賠償や会社の信用問題に発展するケースが相次いでおり，一般企業にも高信頼なシステム開発が求められている．しかし，高信頼ソフトウェア開発手法はその高い開発コストゆえに普及していないのが実情である．このため， MSSS 手法により高信頼ソフトウェア開発を自動化することは，高信頼ソフトウェア開発の導入コストを低減し，それを普及する為にも重要であると考える．また，高信頼ソフトウェア開発の自動化により人間はデバッグやコーディング作業から解放され，より上流工程の創造的作業に専念できると期待できる．

別紙２

論文審査の結果の要旨

学位申請者氏名　　中村　丈洋

審査委員主査　　西野　哲朗

委員　　高橋　治久

委員　　柏原　昭博

委員　　庄野　逸

委員　　寺田　実

委員　　※渡邊　成良

（審査委員署名）

本研究では信頼性を定理証明により定性的に評価可能な高信頼ソフトウェアを形式仕様から自動生成する手法の提案を目的としている．また，この手法の実現にあたり課題となる，高信頼部品整備を容易にするため，既存の高信頼ソフトウェアからソフトウェア部品群を自動生成する手法を提案している．

本論文の構成は、以下の通りである。第１章の序論に続き、第２章では、先行研究として、ソフトウェア開発における信頼性検証、ソフトウェア開発の分業化、自動コード生成、ソフトウェア部品再利用と、B Methodについて紹介されている。続く第３章では、モデル充足ソフトウェア合成フレームワークの概要、構成と運用上の制約が述べられ、第４章で、モデル充足細粒度部品の概要、記述の定義、信頼性の定義と、部品リポジトリについての解説がなされている。第５章では、モデル細分化に関して、非決定的値生成の分離、制約条件展開、操作分割、制約条件抽出、構文要素整列、モデル細分化手法の信頼性保証の概念が説明されている。さらに、第６では、モデル充足ソフトウェア合成について、第７章ではモデル充足細粒度部品生成について述べられており、第８章で手法適用例が示されたのちに、第９章で考察、第１０章で結論が、それぞれ述べられている。

近年のソフトウェアの大規模複雑化に伴い，開発コストの増大と信頼性の低下が問題となっている．高信頼なソフトウェアを容易に開発することはソフトウェア工学の大目標の一つといえる．これに対するドラスティックなアプローチとしては入力仕様や設計から人手によらずコードを生成する自動コード生成が挙げられる．自動コード生成は開発コストの低減や開発期間の短縮だけでなく，人による誤りが混入せず信頼性向上にも寄与する．

本研究では数学を基盤としてソフトウェアの信頼性を定性的に保証する形式手法 B Method の枠組みをソフトウェア部品と再利用の自動化に応用することで，高信頼ソフトウェア部品の自動生成とその再利用による新たなソフトウェア開発手法「モデル充足ソフトウェア合成（MSSS）手法」を提案している．B Method は J.R.Abrial らにより提案された形式手法であり，大きな特徴として数学的仕様と命令型言語による実装間の整合性を定理証明に保証できる点である． MSSS 手法ではこの B Method の信頼性保証の枠組みを応用してモデル充足ソフトウェア部品 (MSFC)を定義する．

MSSS 手法は基盤とする数学的仕様の性質上，集合論と述語論理で記述できる範囲内でしかソフトウェアの仕様を記述できず，非同期処理やユーザインタフェースは自動合成の対象外となる．一方で，ソフトウェアの信頼性と MSFC の信頼性を数学的に定義することで， MSSS 手法では部品生成手法とソフトウェア合成手法の信頼性を数学的に定義でき，定性的な評価が可能である．本研究ではソフトウェア部品の生成手法自体に定理証明を適用し，その信頼性を定性的に保証する事を試みた．これにより，細分化モデルの信頼性を保証するのに必要な推論器の性質と，制約条件の抽出条件を定理証明により得られた．ソフトウェア合成についても提案した合成手順で部品の実装間の制約条件の矛盾以外は保証できることを示し，合成結果に矛盾が生じた際の低コストな解決手段を提案した．

MSSS 手法のように数学的判定を必要とする部品自動再利用では膨大な部品群に対して数学的判定を行うため，計算コストの低減が問題となる．本研究ではこの問題に対して，数学的に意味の等しい数学的仕様の字面が一致し，また，含意関係となる字面が完全部分一致となるようモデル細分化手法を提案した．これにより，文字列一致による効率的な部品検索を可能にした．

本研究では MSSS 手法の適用例として銀行口座システムなどに対する MSFC 生成とレンタカーシステムなどの自動合成を行った．これにより生成された MSFC やソフトウェアに対して B Method の証明器を適用し，定義どおりの信頼性が得られることを確認した．ただし， B Method により記述されたソフトウェアは現状では広く公開されておらず，より実践的な手法の適用が今後の課題となる．

近年では，システムの不具合が莫大な賠償や会社の信用問題に発展するケースが相次いでおり，一般企業にも高信頼なシステム開発が求められている．しかし，高信頼ソフトウェア開発手法はその高い開発コストゆえに普及していないのが実情である．このため， MSSS 手法により高信頼ソフトウェア開発を自動化することは，高信頼ソフトウェア開発の導入コストを低減し，それを普及する為にも重要であると考える．また，高信頼ソフトウェア開発の自動化により人間はデバッグやコーディング作業から解放され，より上流工程の創造的作業に専念できると期待できる．

よって、本論文は博士（工学）の学位論文として十分な価値を有するものと認める。